ISSN 1995-0802, Lobachevskii Journal of Mathematics, 2018, Vol. 39, No. 7, pp. 985–991. © Pleiades Publishing, Ltd., 2018.

Polynomial Greatest Common Divisor as a Solution of System of Linear Equations

D. A. Dolgov*

(Submitted by F. M. Ablayev)

Department of System Analysis and Information Technologies,
Institute of Computational Mathematics and Information Technologies,
Kazan (Volga Region) Federal University, ul. Kremlevskaya 18, Kazan, Tatarstan, 420008 Russia

Received December 6, 2017

Abstract—In this article we present a new algebraic approach to the greatest common divisor (GCD) computation of two polynomials based on Bezout's identity. This approach is based on the solution of system of linear equations. Also we introduce the dmod operation for polynomials. This operation on polynomials f, g is used to reduce the degree of the larger polynomial f in a finite field F_p. This operation saves $GCD(f, g)$. Also we present some ideas how to reduce spurious factors that arise at the procedure.

DOI: 10.1134/S1995080218070090

Keywords and phrases: *Polynomial GCD, Euclidean algorithm, system of linear equations, generalized Schur algorithm.*

1. INTRODUCTION

Polynomials have been studying for a very long time. A whole series of objects is connected with polynomials: zero, negative, complex numbers, the emergence of the theory of groups as a section of mathematics and the allocation of classes of special functions in analysis. More applications are found for polynomials of one variable.

Computation of greatest common divisor (GCD) of polynomials of one variable can be implemented like as the GCD computation for integer numbers by the Euclid GCD algorithm using operation of division at long integers. The polynomial GCD has specific properties that make it a fundamental notion in various areas of algebra. Often the roots of GCD of two polynomials are common roots of the two polynomials, and this allows us to get information of the roots without computing them. Some results concerning theory of polynomials can be found in [1–3, 6]. Computation of GCD of two polynomials can be used in cryptography (public key cryptography by the means of elliptic curves), finite fields, computer algebra, coding theory (cyclic redundancy codes and BCH codes). In particular it can be used in polynomial factorisation problem.

In this article we present a new algebraic approach to the GCD computation of two polynomials of one variable based on Bezout's identity. This approach is based on the solution of system of linear equations. So, we turn from the problem of GCD computation to the problem of solving a system of linear equations. Also we present the dmod operation on polynomials f, g, which is used to reduce the degree of the larger polynomial f in a finite field F_p. Also we present some ideas how to reduce spurious factors that arise at the procedure.

*E-mail: Dolgov.kfu@gmail.com